DIGIPASS CertiID

Installation Guide

3.1.0

Disclaimer of Warranties and Limitations of Liabilities

The Product is provided on an 'as is' basis, without any other warranties, or conditions, express or implied, including but not limited to warranties of merchantable quality, merchantability of fitness for a particular purpose, or those arising by law, statute, usage of trade or course of dealing. The entire risk as to the results and performance of the product is assumed by you. Neither we nor our dealers or suppliers shall have any liability to you or any other person or entity for any indirect, incidental, special or consequential damages whatsoever, including but not limited to loss of revenue or profit, lost or damaged data of other commercial or economic loss, even if we have been advised of the possibility of such damages or they are foreseeable; or for claims by a third party. Our maximum aggregate liability to you and that of our dealers and suppliers shall not exceed the amount paid by you for the Product. The limitations in this section shall apply whether or not the alleged breach or default is a breach of a fundamental condition or term, or a fundamental breach. Some states/countries do not allow the exclusion or limitation or liability for consequential or incidental damages so the above limitation may not apply to you.

Copyright

Trademarks

VASCO, VACMAN, IDENTIKEY, aXsGUARD, DIGIPASS and the Vasco ‘V’ logo are either registered or unregistered trademarks of VASCO Data Security, Inc. and/or VASCO Data Security International GmbH in the U.S. and other countries.

Version: 2009-06-16

Table of Contents

Illustration Index

Index of Tables

1 Introduction

This document provides you the information you will need to install DIGIPASS CertiID. It will guide you through preparation, installation, and post-installation tasks, which may be required for your system.

For detailed instructions and background information refer to other user documentation available on the product CD.

This manual provides information about how to:

- Verify system requirements and prepare a typical installation of DIGIPASS CertiID
- Perform a typical installation of DIGIPASS CertiID
- Remove, repair, or modify a typical DIGIPASS CertiID installation

This manual does **not** provide:

- a detailed introduction to DIGIPASS CertiID, its features, and components (refer to DIGIPASS CertiID User Manual)
- detailed instructions about using and configuring DIGIPASS CertiID applications (refer to DIGIPASS CertiID User Manual)
- detailed instructions about using DIGIPASS CertiID with common third-party applications (refer to DIGIPASS CertiID Getting Started Manual)

2 Requirements

This chapter gives an overview of the DIGIPASS CertiID system requirements.

It covers the following topics:

- Operating System Requirements
- General Requirements
- Software Requirements

2.1 Operating System Requirements

To install DIGIPASS CertiID software you need:

- Microsoft Windows Vista with SP1, 32-bit / 64-bit
- Microsoft Windows XP with SP2 (or higher), 32-bit
- Microsoft Windows 2000 with SP4 (or higher)
- Microsoft Windows Server 2008 with SP1 (or higher), 32-bit / 64-bit
- Microsoft Windows Server 2003 with SP1 (or higher), 32-bit / 64-bit

2.2 General Requirements

To use DIGIPASS CertiID software you need:

- a supported smart card reader with PC/SC compatible driver, e.g. DP905
  the smart card reader needs to support extended APDUs (to generate 2048 bit keys and other operations)
- a supported smart card or token, e.g. DP860
- a PC with 400 MHz processor clock speed
- 256 MB RAM or higher recommended
- 150 MB of free disk space

DIGIPASS CertiID software supports smart cards and tokens based on:

- Siemens CardOS 4.01A
- Siemens CardOS 4.3B
- Giesecke & Devrient STARCOS 3.1
- Oberthur ID One Cosmo

Supported tokens include:

- VASCO DP860
- VASCO DP KEY 1

2.3 Software Requirements

DIGIPASS CertiID software supports the following certification authorities (CA):

- Windows Certification Authority
- Entrust Certification Authority
- any certification authority based on X.509 v3 certificates

DIGIPASS CertiID software supports all third-party applications based on PKCS#11 Version 2.2 and Microsoft Cryptography API, including Cryptography API: Next Generation (CNG) for Microsoft Windows Vista.

Installing DIGIPASS CertiID

This chapter outlines the preparation that you need to do before installing DIGIPASS CertiID and describes how to perform a typical DIGIPASS CertiID software installation.

It covers the following topics:

- Pre-Installation Settings and Tasks
- Installation Overview
- Installing DIGIPASS CertiID Software
- Installing DIGIPASS CertiID Software (Silently)

2.4 Pre-Installation Settings and Tasks

2.4.1 Administrator privileges

To install DIGIPASS CertiID you need to be logged on with a user that has local administrator privileges.

2.4.2 Smart card reader drivers

Before you install and use DIGIPASS CertiID, your smart card reader or token must be installed and fully operative.

2.4.3 DIGIPASS Secure Authentication Suite (SAS)

If you have DIGIPASS Secure Authentication Suite (SAS) installed, you need to uninstall it first, before installing DIGIPASS CertiID.

2.4.4 URL for update client

DIGIPASS CertiID includes an update client application that searches for software updates on the Internet. By default, it searches on a pre-defined VASCO update server. However, if you need to set the update URL to an internal Web server, because you don't want to allow client machines to connect to the Internet, you can change it directly in the installation package using any MSI editing software, such as Microsoft Orca.

The URL for the update client is stored in the Registry table under the following key:

- Registry: registry4.58949955_0765_4225_AB94_EA84F43B417A
- Name: SettingsURL

You can also change the URL, if DIGIPASS CertiID is already installed, via the string value SettingsURL under the following Windows Registry key:

[HKLM\SOFTWARE\Wise Solutions\WiseUpdate\Apps\VASCO DIGIPASS CertiID]

2.5 Installation Overview

1. Verify that you have the necessary system components installed.
2. If required, upgrade your system to the latest service pack version.
3. If required, install desired third-party software products.
4. Install your smart card reader and/or token devices.
5. Install DIGIPASS CertiID software.

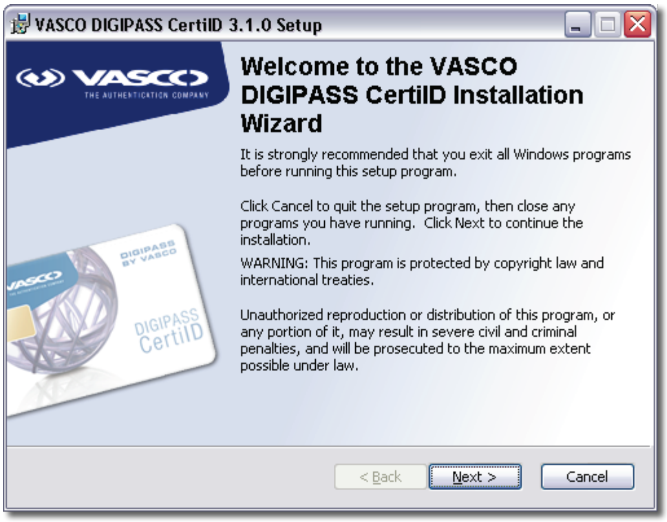
2.6 Installing DIGIPASS CertiID Software

➢ To install DIGIPASS CertiID software

1. Insert the DIGIPASS CertiID product CD and select **Setup and Installation > Install DIGIPASS CertiID** from the CD start menu to launch the setup program.

TIP
If the CD start menu does not appear automatically, you might have the *AutoPlay* feature for your CD/DVD-ROM deactivated. In this case, you can start the CD start menu manually by launching autorun.exe in the CD main directory!

NOTE
If you want or need to launch the setup program directly, you can find it in the Install directory of your DIGIPASS CertiID product CD. The 32-bit version of the setup is setup.msi; the 64-bit version is setup64.msi.


VASCO DIGIPASS CertiID 3.1.0 Setup

Welcome to the VASCO DIGIPASS CertiID Installation Wizard

It is strongly recommended that you exit all Windows programs before running this setup program.

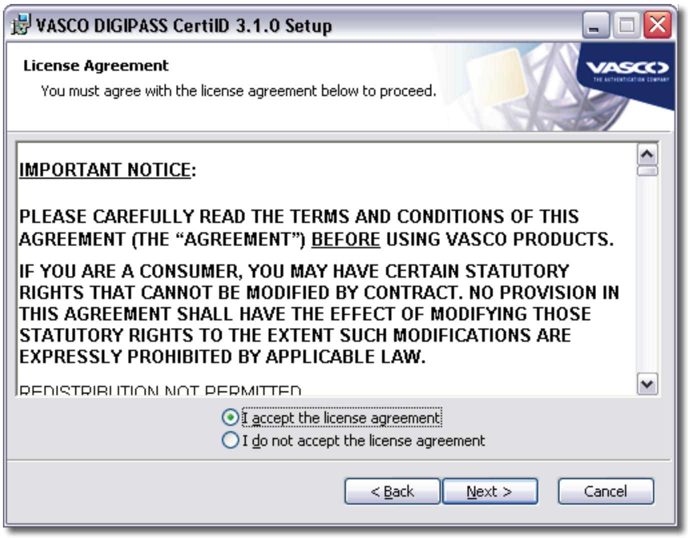
Click Cancel to quit the setup program, then close any programs you have running. Click Next to continue the installation.

WARNING: This program is protected by copyright law and international treaties.

Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under law.

Figure 1: Installing DIGIPASS CertiID (1)

2. Read the license agreement text, select **I accept the license agreement** and click **Next**.



VASCO DIGIPASS CertiID 3.1.0 Setup

License Agreement

You must agree with the license agreement below to proceed.

IMPORTANT NOTICE:

PLEASE CAREFULLY READ THE TERMS AND CONDITIONS OF THIS AGREEMENT (THE "AGREEMENT") BEFORE USING VASCO PRODUCTS.

IF YOU ARE A CONSUMER, YOU MAY HAVE CERTAIN STATUTORY RIGHTS THAT CANNOT BE MODIFIED BY CONTRACT. NO PROVISION IN THIS AGREEMENT SHALL HAVE THE EFFECT OF MODIFYING THOSE STATUTORY RIGHTS TO THE EXTENT SUCH MODIFICATIONS ARE EXPRESSLY PROHIBITED BY APPLICABLE LAW.

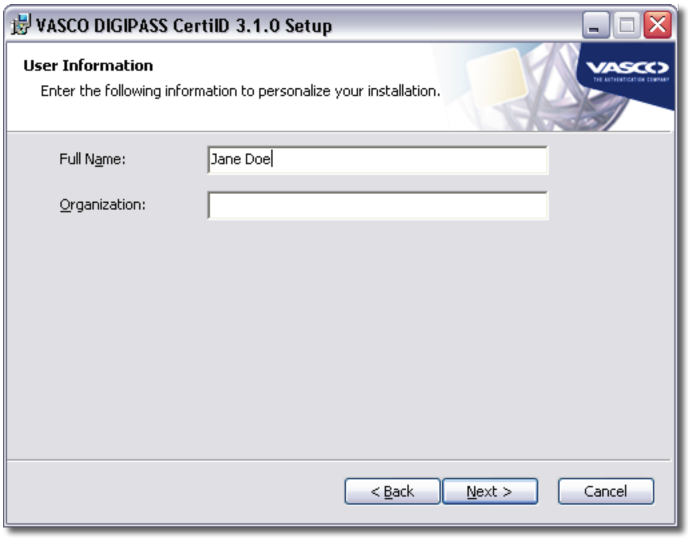
REDISTRIBUTION NOT PERMITTED

● I accept the license agreement

○ I do not accept the license agreement

Figure 2: Installing DIGIPASS CertiID (2) – Accepting License Agreement

3. Enter your name and the name of your organization to personalize your copy.



VASCO DIGIPASS CertiID 3.1.0 Setup

User Information

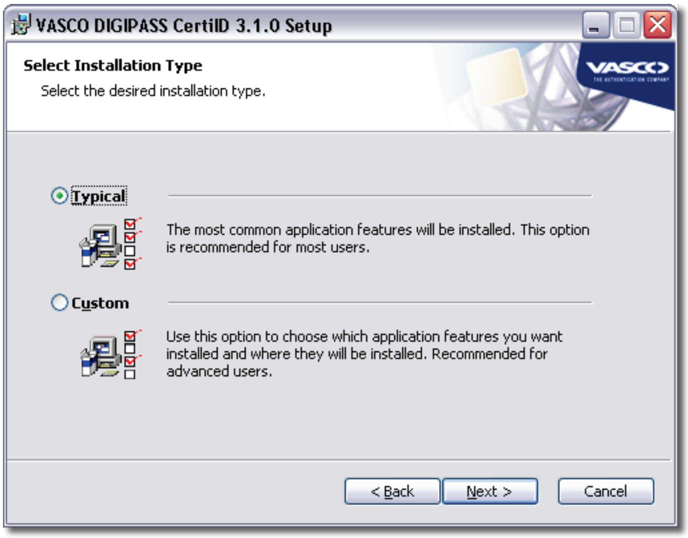
Enter the following information to personalize your installation.

Full Name: Jane Doe

Organization:

Figure 3: Installing DIGIPASS CertiID (3) – Specifying User Information

4. Select the desired installation type.



VASCO DIGIPASS CertiID 3.1.0 Setup

Select Installation Type

Select the desired installation type.

● Typical

The most common application features will be installed. This option is recommended for most users.

○ Custom

Use this option to choose which application features you want installed and where they will be installed. Recommended for advanced users.

Figure 4: Installing DIGIPASS CertiID (4) – Selecting Installation Type

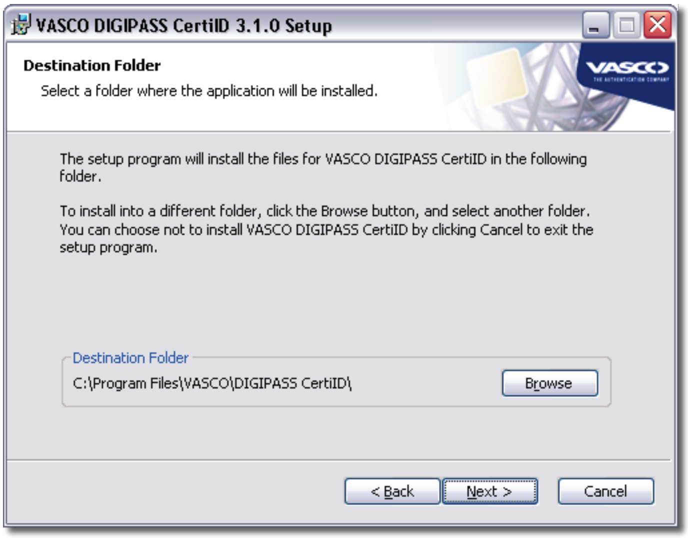
- Select **Typical**, if you want to install the most common applications features automatically. Continue with Step 8.

  A typical installation installs both, **VASCO CertiID Smart Card Crypto Provider** and **VASCO Card Module** on a machine. If you install on Windows XP or Windows 2000 the former is registered as default cryptographic provider, if you install on Windows Vista the latter is registered.

- Select **Custom**, if you want to choose and configure the application features to be installed yourself. Continue with the next step.

5. Select the destination folder for the installation.

   The default destination folder is C:\Program Files\VASCO\DIGIPASS CertiID\.



VASCO DIGIPASS CertiID 3.1.0 Setup

Destination Folder

Select a folder where the application will be installed.

The setup program will install the files for VASCO DIGIPASS CertiID in the following folder.

To install into a different folder, click the Browse button, and select another folder. You can choose not to install VASCO DIGIPASS CertiID by clicking Cancel to exit the setup program.

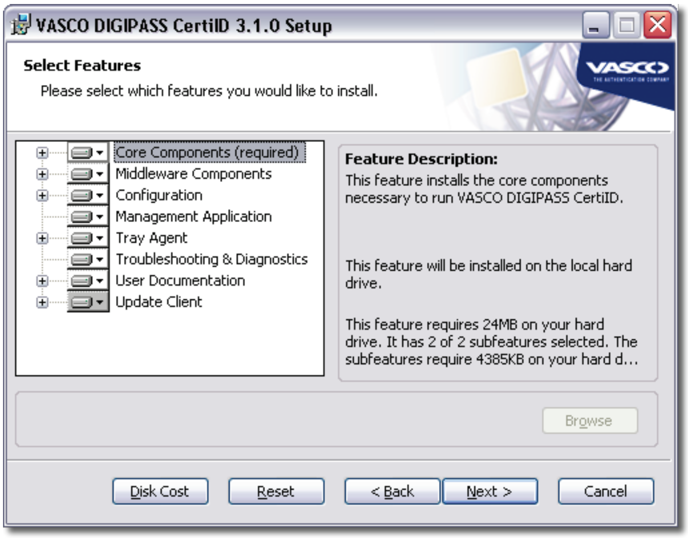
Destination Folder

C:\Program Files\VASCO\DIGIPASS CertiID\

Figure 5: Installing DIGIPASS CertiID (5) – Selecting Destination Folder

> NOTE
>
> The 64-bit version of DIGIPASS CertiID installs 64-bit and some 32-bit components. If you install it, you can only select the destination folder for the 64-bit components; 32-bit components are always installed to the default destination folder.

6. Select the software modules you want to install on your machine.



VASCO DIGIPASS CertiID 3.1.0 Setup

Select Features

Please select which features you would like to install.

- Core Components (required)
- Middleware Components
- Configuration
- Management Application
- Tray Agent
- Troubleshooting & Diagnostics
- User Documentation
- Update Client

Feature Description:

This feature installs the core components necessary to run VASCO DIGIPASS CertiID.

This feature will be installed on the local hard drive.

This feature requires 24MB on your hard drive. It has 2 of 2 subfeatures selected. The subfeatures require 4385KB on your hard d...

Figure 6: Installing DIGIPASS CertiID (6) – Selecting Features

Feature	Purpose
Core Components	Contains all core components needed to run DIGIPASS CertiID, including token drivers. NOTE: This feature is required to be installed!
Token Drivers	Installs token drivers for supported tokens. NOTE: This feature does **not** install hardware drivers!
Token Templates	Installs token templates required to initialize empty tokens.
PKI Middleware Components	This includes all cryptographic middleware modules.
Cryptographic Service Provider (CSP)	Installs VASCO CertiID Smart Card Crypto Provider for cryptographic support for Microsoft and other CryptoAPI aware products.
PKCS#11 Module	Installs cryptographic support for Mozilla and other PKCS#11 aware products.
Entrust Configuration	Registers the DP CertiID PKCS#11 Library with Entrust clients. NOTE: If you select this feature, but no entrust configuration file (i.e. entrust.ini) is found, it is automatically deselected and not installed!
Firefox/Thunderbird Configuration	Installs a Mozilla extension that automatically registers the DP CertiID PKCS#11 Library with Mozilla Firefox and Mozilla Thunderbird for each user when the applications are started the first time.
Card Module	Installs VASCO Card Module. NOTE: Requires Microsoft Base Smart Card Crypto Provider to work (not available for Microsoft Windows 2000)!
IdenTrust	Installs support libraries for IdenTrust.
ISPI (for Mozilla Firefox)	Installs Mozilla Firefox plug-in to support IdenTrust Signing Plug-In (ISPI) specification.
ISPI (for Microsoft Internet Explorer)	Installs an ActiveX control for Microsoft Internet Explorer to support IdenTrust Signing Plug-In (ISPI) specification.
ISIL (for Java-capable browsers)	Installs a Java executable to support IdenTrust Signing Interface Library (ISIL) specification within Java-capable Web browsers. NOTE: Requires an installed Java Runtime Environment (JRE) to work! Currently, only 32-bit is supported!
Configuration	Installs tools to configure DIGIPASS CertiID.
Configuration Center	Installs the basic configuration center.
Group Policy Administrative Templates	Installs Administrative Templates to configure DIGIPASS CertiID via Group Policy.
Management Application	Installs the DP CertiID Management Application, used to manage tokens and digital certificates.
Tray Agent	Installs the DP CertiID Tray Agent, used for automatic registration of certificates.
Certificate Registration Plug-in	Installs plug-in for DP CertiID Tray Agent to register and unregister digital certificates automatically.

Feature	Purpose
Slot and Token Plug-in	Installs plug-in for DP CertiID Tray Agent to monitor and indicate the state of your slots and tokens.
Troubleshooting and Diagnostics Plug-in	Installs plug-in for DP CertiID Tray Agent to monitor the state of system and user diagnostics.
Troubleshooting and Diagnostics	Installs programs used to diagnose and troubleshoot issues with the middleware.
User Documentation	Installs end user documentation and online help files in different languages. By default, only English documentation is installed.
Update Client	Installs an update application to search for software updates on the Internet.

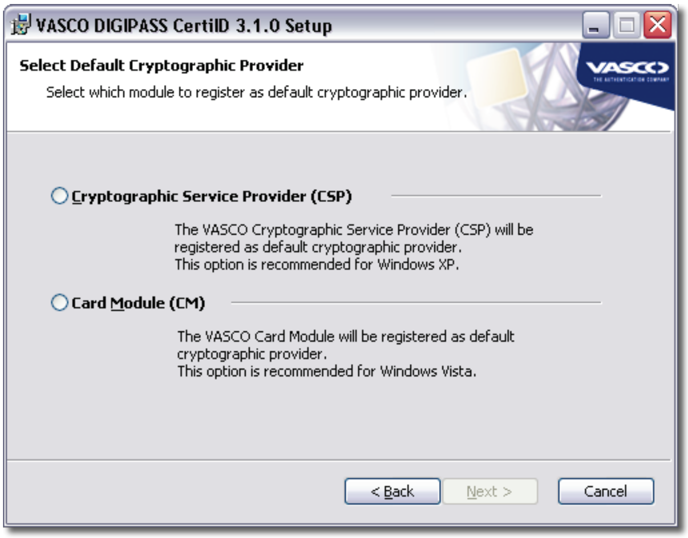
Table 1: DIGIPASS CertiID Program Features

NOTE
The Entrust Client reads its configuration file only once, i.e. when it starts. If you select the Entrust Configuration feature, the new configuration settings do not become effective, until you reboot the machine after installing DIGIPASS CertiID.

NOTE
The ISIL support library is installed to the lib/ext directory of all installed Java Runtime Environments (JRE) found. If you install a new version of JRE, you can renew the ISIL library installation by executing VdsISILReg32.exe in the DIGIPASS CertiID program directory.

7. If required, select which module to register as default cryptographic provider.

   This step is only required, if you install both, **VASCO CertiID Smart Card Crypto Provider** and **VASCO Card Module** on a machine, where the Microsoft Base Smart Card Crypto Provider is available. **Microsoft Base Smart Card Crypto Provider** is not available for Microsoft Windows 2000!


VASCO DIGIPASS CertiID 3.1.0 Setup

Select Default Cryptographic Provider

Select which module to register as default cryptographic provider.

○ Cryptographic Service Provider (CSP)

The VASCO Cryptographic Service Provider (CSP) will be registered as default cryptographic provider.
This option is recommended for Windows XP.

○ Card Module (CM)

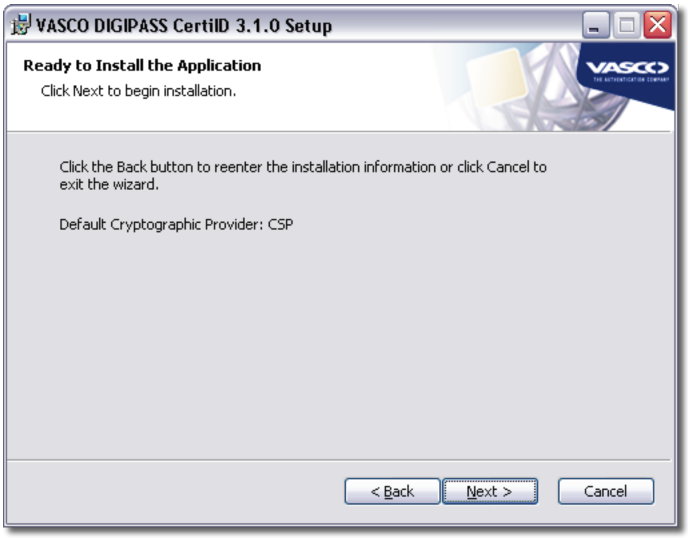
The VASCO Card Module will be registered as default cryptographic provider.
This option is recommended for Windows Vista.

Figure 7: Installing DIGIPASS CertiID (7) – Selecting Default Cryptographic Provider

- Select **Cryptographic Service Provider (CSP)**, if you want to register VASCO CertiID Smart Card Crypto Provider as default cryptographic provider.
- Select **Card Module**, if you want to register VASCO Card Module as default cryptographic provider.

> NOTE
> Microsoft Windows allows only one module being registered as default cryptographic provider module. The default cryptographic provider is linked with the supported smart card and token types and is automatically used by all applications using CAPI for cryptographic operations.
>
> This setting does not affect applications supporting PKCS#11.

8. Click **Next** to start installation.



VASCO DIGIPASS CertiID 3.1.0 Setup

Ready to Install the Application

Click Next to begin installation.

Click the Back button to reenter the installation information or click Cancel to exit the wizard.

Default Cryptographic Provider: CSP

Figure 8: Installing DIGIPASS CertiID (8) – Ready To Install

9. After successful installation, click **Finish** to exit the setup program.

2.7 Installing DIGIPASS CertiID Software (Silently)

You can install the DIGIPASS CertiID software silently (without setup GUI) using the following command line:

```
msiexec /i setup.msi /qn [PROPERTY=VALUE]
```

where PROPERTY can be the name of a property to be set to VALUE.

2.7.1 Supported properties

Property	Description
ADDLOCAL	Specifies which program features should be installed. The features are specified in a comma separated list. If you use this property, you need to specify all program features you want to install. NOTE: If you mistype a feature value, you will receive an error message! Possible values: VdsCore …install DP CertiID Core Components (required!) VdsCardModule …install VASCO Card Module VdsConfig …install DP CertiID Configuration Center VdsCPCertReg …install “Certificate Registration” plug-in for DP CertiID Tray Agent VdsCPDiag …install “Troubleshooting and Diagnostics” plug-in for DP CertiID Tray Agent VdsCPSlotToken …install “Slot and token” plug-in for DP CertiID Tray Agent VdsCSP …install VASCO CertiID Smart Card Crypto Provider VdsDiag …install DP CertiID Troubleshooting and Diagnostics VdsDocumentationEnglish …install English documentation VdsGroupPolicy …install Group Policy Administrative Templates VdsIdentrustISIL …install IdenTrust support for Java-capable browsers (ISIL) VdsIdentrustISPIIE …install IdenTrust support for Microsoft Internet Explorer (ISPI) VdsIdentrustISPIMoz …install IdenTrust support for Mozilla Firefox (ISPI) VdsPKCS11 …install the DP CertiID PKCS#11 Library VdsPKCS11ConfigEntrust …register DP CertiID PKCS#11 Library with Entrust clients VdsPKCS11ConfigFirefox …register DP CertiID PKCS#11 Library with Mozilla Firefox and Mozilla Thunderbird VdsPKIMan …install DP CertiID Management Application VdsTokDriversCardos4 …install token drivers for CardOS 4.01A and 4.3B tokens VdsTokDriversIdOne …install token drivers for CertiID ID-One tokens VdsTokDriversStarcos3 …install token drivers for STARCOS 3.x tokens VdsTokTemplates …install token templates required to initialize empty tokens VdsTray …install DP CertiID Tray Agent VdsUpdateClient …install update application VdsUpdateClientAuto …automatically start update application on system start

Property	Description
DEFAULTPROVIDER	Specifies which module to register as default cryptographic provider. Possible values: Auto …automatically determine module to register (default) CSP …registers VASCO CertiID Smart Card Crypto Provider CM …registers VASCO Card Module

Table 2: Installation Properties

NOTE
Property names and values are case sensitive.

2.7.2 Examples

This example performs a typical installation with the default program features and automatically registers the correct default cryptographic provider:

```
msiexec /i setup.msi /qn
```

This example installs a minimum set required to run DIGIPASS CertiID with third-party applications:

```
msiexec /i setup.msi /qn
ADDLOCAL=VdsCore,VdsCSP,VdsCardModule,VdsPKCS11,VdsTokDriversCardos4,
VdsTokDriversIdOne,VdsTokDriversStarcos3
```

This example installs all features and registers VASCO Card Module as default cryptographic provider:

```
msiexec /i setup.msi /qn DEFAULTPROVIDER=CM ADDLOCAL=ALL
```

2.8 Post-Installation Settings and Tasks

2.8.1 Installing Group Policy Administrative Templates on Domain Controller

If you want to use domain Group Policy, but don't want to install DIGIPASS CertiID on the domain controller, you need to copy the Administrative Templates to the respective directories.

The plain Administrative Templates are on the DIGIPASS CertiID product CD in the Install\Group Policy folder.

- For Windows Server 2008 copy VascoDPCertiID.admx and en-US\VascoDPCertiID.adml to <WindowsFolder>\PolicyDefinitions, respectively, where <WindowsFolder> is the full path to your Windows folder, e.g. C:\Windows\.
- For Windows Server 2003 copy VascoDPCertiID.adm to <SystemFolder>\GroupPolicy\Adm, where <SystemFolder> is the full path to your system folder, e.g. C:\Windows\System32\.

2.8.2 Registering the DP CertiID PKCS#11 Library in Mozilla Firefox and Mozilla Thunderbird

If you want to use the **DP CertiID PKCS#11 Library** in **Mozilla Firefox** or **Mozilla Thunderbird**, respectively, you need to register it in that applications.

If you select the Firefox/Thunderbird Configuration feature when installing DIGIPASS CertiID, a Mozilla extension is installed and registered. This extension is launched for each user once, when the Mozilla application is started asking wheter to register the DP CertiID PKCS#11 Library automatically.

The extension also adds two commands to the **Tools** menu of the Mozilla applications, i.e. **Register VASCO DP CertiID PKCS#11** and **Unregister VASCO DP CertiID PKCS#11**, allowing to conveniently register and unregister the DP CertiID PKCS#11 Library, respectively.

For information about how to manually register/unregister the DP CertiID PKCS#11 Library in Mozilla applications, refer to the DIGIPASS CertiID Getting Started Manual.

3 Removing/Repairing/Modifying DIGIPASS CertiID

This chapter describes how to remove an existing DIGIPASS CertiID installation, add or remove single components, or to repair an installation, if files have been corrupted, deleted, or lost.

It covers the following topics:

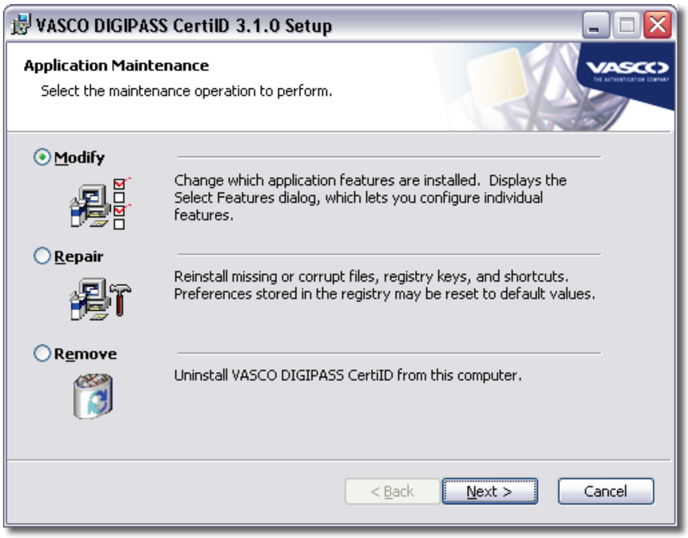
- Removing/Repairing/Modifying DIGIPASS CertiID

3.1 Removing/Repairing/Modifying DIGIPASS CertiID

➢ To remove/repair/modify an existing DIGIPASS CertiID installation

1. Open the control panel via **Start > Settings > Control Panel**.
2. Double-click **Add and Remove Programs**.
3. Select VASCO DIGIPASS CertiID and click **Change**.

   The **Application Maintenance Windows** appears.



VASCO DIGIPASS CertiID 3.1.0 Setup

Application Maintenance

Select the maintenance operation to perform.

● Modify

Change which application features are installed. Displays the Select Features dialog, which lets you configure individual features.

○ Repair

Reinstall missing or corrupt files, registry keys, and shortcuts. Preferences stored in the registry may be reset to default values.

○ Remove

Uninstall VASCO DIGIPASS CertiID from this computer.

Figure 9: Selecting Maintenance Operation

4. Do one of the following:

   (a) If you want to remove the software from you system, select **Remove** and click **Next**.

   (b) If you want to repair a corrupted or damaged installation, select **Repair** and click **Next**.

   (c) If you want to remove or install additional components select **Modify** and click **Next**.

NOTE
If you want to perform certificate-based authentication to the operating system, you need to restart the machine first, after changing the registered default cryptographic provider via **Modify**!